PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-223787
(43)Date of publication of application : 13.08.1992

(51)Int.Cl. H04N 7/167
H04H 1/00
H04L 9/28

(21)Application number : 03-087371
(22)Date of filing : 28.03.1991

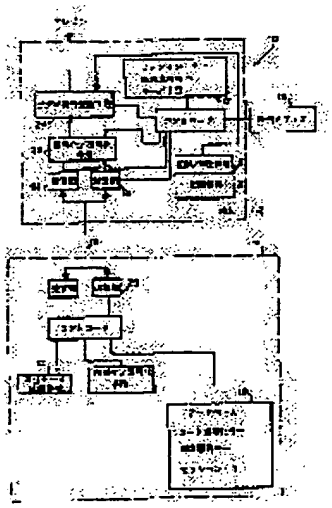
(71)Applicant : GTE LAB INC
(72)Inventor : WALKER STEPHEN S
SIDLO CLARENCE M
TEARE MELVIN J

(30)Priority

Priority number	Priority date	Priority country
90 501620	29.03.1990	US
90 501682	29.03.1990	
90 501683	29.03.1990	US
90 501684	29.03.1990	
90 501685	29.03.1990	US
90 501688	29.03.1990	
		US
		US
		US

(54) VIDEO CONTROL SYSTEM

(57)Abstract:
PURPOSE: To provide a video control system for decoding the recording copy of an enciphered broadcasting or video image to control viewing.
CONSTITUTION: A video program including a 1st field including both a random digital code enciphered by a code cryptographic key and program identification data and a 2nd field including an unviewable video signal previously converted from a viewable video signal by that random digital code is provided to a terminal by a video program means. The terminal transmits the program identification data to a central mechanism. The central mechanism retrieves one code cryptographic key at least corresponding to the program identification data and transmits that key to the terminal. The terminal receives the code cryptographic key, decodes the digital code enciphered by the code cryptographic key in the 1st frame and converts the unviewable video signal in the 2nd frame into the viewable video signal while using the deciphered random digital code.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the

(19)日本国特許庁（ＪＰ）　(12)公開特許公報(A)　(11)特許出願公開番号

特開平4－223787

(43)公開日　平成4年(1992)8月13日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｎ　7/167		8324－5C		
Ｈ０４Ｈ　1/00		Ｆ　7240－5K		
Ｈ０４Ｌ　9/28				
		7117－5K	Ｈ０４Ｌ　9/02	Ａ

審査請求　未請求　請求項の数14(全　7　頁)

(21)出願番号　特願平3－87371

(22)出願日　平成３年(1991)３月28日

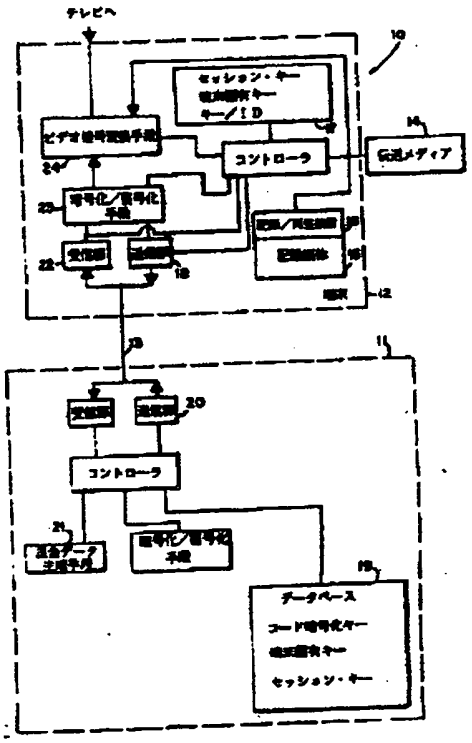
(31)優先権主張番号　５０１６２０
(32)優先日　1990年３月29日
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　５０１６８２
(32)優先日　1990年３月29日
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　５０１６８３
(32)優先日　1990年３月29日
(33)優先権主張国　米国（ＵＳ）

(71)出願人　591003415
ジー・テイー・イー・ラボラトリーズ・インコーポレイテツド
アメリカ合衆国19801デラウエア州ウイルミントン、オレンジ・ストリート1209
(72)発明者　ステイーブン・エス・ウオーカー
米国マサチユーセツツ州マールボロ、ケレハー・ロード117
(72)発明者　クラレンス・エム・シドロー
米国マサチユーセツツ州フラミンガム、ロウリー・ロード５
(74)代理人　弁理士　倉内　基弘　（外１名）

最終頁に続く

(54)【発明の名称】　ビデオ制御システム

(57)【要約】　（修正有）
【目的】　視聴することが制御されるような、暗号化された放送またはビデオ画像の収録複写物を復号化するビデオ制御システムを提供する。
【構成】　ビデオ番組手段が、コード暗号化キーによって暗号化されたランダムディジタルコードと、番組識別データの両方を含む第１フィールドと、そのランダムディジタルコードによって前もって視聴できるビデオ信号から変換された視聴できないビデオ信号を含む第２フィールドと、を含むビデオ番組を端末に提供する。端末は、番組識別データを中央機構に送信する。中央機構は、番組識別データに対応する少なくとも１つのコード暗号化キーを検索し、端末へ送信する。端末は、コード暗号化キーを受信し、コード暗号化キーによって暗号化された第１フレームのディジタルコードを復号化し、復号化されたランダムディジタルコードを用いて第２フレームの視聴できないビデオ信号を視聴できるビデオ信号に変換する。



1

【特許請求の範囲】

【請求項1】　中央機構と、端末と、コード暗号化キーによって暗号化されたランダムディジタルコードと番組識別データとを含む第1フィールドと、前記ランダムディジタルコードによって視聴できるビデオ信号から前もって変換された視聴できないビデオ信号を含む第2フィールドと、を含む一連のテレビジョンフィールドを含むビデオ番組を前記端末に提供するビデオ番組手段と、を備え、前記端末が、前記番組識別データを前記中央機構に送信する手段を含み、前記中央機構が、番組識別データに対応する少なくとも1つのコード暗号化キーを格納しそして検索するデータベースと、前記中央機構から前記端末へ前記コード暗号化キーを送信する手段と、を含み、前記端末が、さらに、前記中央機構からコード暗号化キーを受信する手段と、前記コード暗号化キーによって前記第1フィールドの暗号化されたディジタルコードを復号化する復号化手段と、前記復号化されたランダムディジタルコードを用いて前記第2フィールドの前記視聴できないビデオ信号を前記視聴できるビデオ信号に変換する手段と、を含む、ビデオ制御システム。

【請求項2】　1つの番組に対して複数のコード暗号化キーが使用され、所望するコード暗号化キーが、前記所望するコード暗号化キーによって暗号化されたランダムディジタルコードに対応するコード暗号化キー識別データによって前記複数のコード暗号化キーから選択される、請求項1記載のビデオ制御システム。

【請求項3】　前記ビデオ番組手段が前記番組を前記端末に転送する手段である、請求項1記載のビデオ制御システム。

【請求項4】　前記転送する手段がＣＡＴＶシステムである請求項3記載のビデオ制御システム。

【請求項5】　前記端末が、さらに、端末識別データと端末に特定の暗号化キーを記憶する手段と、前記端末識別データを前記番組識別データとともに前記中央機構に送信する手段と、を含み、前記中央機構が、さらに、前記端末に特定の暗号化キーの複製を記憶する手段と、前記端末に特定の暗号化キーによって前記コード暗号化キーを暗号化する手段と、前記中央機構から前記端末に前記暗号化されたコード暗号化キーを送信する手段と、を含み、前記端末が、さらに、前記中央機構から前記暗号化されたコード暗号化キーを受信する手段と、前記端末に特定の暗号化キーによって前記コード暗号化キーを復号化する復号化手段と、を含む、請求項1記載のビデオ制御システム。

【請求項6】　前記端末が、前記端末に特定の暗号化キーによって前記端末識別データを暗号化する手段と、前記中央機構に暗号化されない端末識別データと暗号化された端末識別データとを送信する手段と、を含み、前記中央機構が、暗号化されない端末識別データと暗号化された端末識別データとを比較して端末の同一性を検証する手段を含む、請求項5記載のビデオ制御システム。

2

【請求項7】　前記中央機構が、さらに、前記端末識別データと前記番組識別データとに基づいて課金データを生成する手段を含む、請求項5記載のビデオ制御システム。

【請求項8】　前記端末が、さらに、端末識別データと端末に特定の暗号化キーとを記憶する手段と、前記中央機構に前記番組識別データと前記端末識別データとを送信する手段と、を含み、前記中央機構が、さらに、セッション暗号化キーを提供する手段と、前記端末に特定の暗号化キーによって前記セッション暗号化キーを暗号化する手段と、前記中央機構から前記端末へ前記暗号化されたセッション暗号化キーを送信する手段と、前記暗号化されたセッション暗号化キーによって前記コード暗号化キーを暗号化する手段と、前記中央機構から前記端末に前記暗号化されたコード暗号化キーを送信する手段と、を含み、前記端末が、さらに、前記中央機構からの暗号化されたセッション暗号化キーを受信する手段と、前記端末に特定の暗号化キーによって前記セッション暗号化キーを復号化する復号化手段と、前記中央機構からの暗号化されたコード暗号化キーを受信するための手段と、前記セッション暗号化キーによって前記コード暗号化キーを復号化する復号化手段と、を含む、請求項1記載のビデオ制御システム。

【請求項9】　前記端末が、前記端末に特定の暗号化キーによって前記端末識別データを暗号化する手段と、前記中央機構に暗号化されない端末識別データと暗号化された端末識別データとを送信する手段と、を含み、前記中央機構が、暗号化されない端末識別データと暗号化された端末識別データとを比較して端末の同一性を検証する手段を含む、請求項8記載のビデオ制御システム。

【請求項10】　前記中央機構が、さらに、前記端末識別データと前記番組識別データとに基づいて課金データを生成する手段を含む、請求項8記載のビデオ制御システム。

【請求項11】　前記ビデオ番組手段が、前記端末に配置されて前記番組に記録されるビデオ収録画像を再生する手段である、請求項1記載のビデオ制御システム。

【請求項12】　コード暗号化キーによって暗号化されたランダムディジタルコードと番組識別データの両方を含む第1フィールドと、視聴可能なビデオ信号から前記ランダムディジタルコードによって前もって変換された視聴不可能なビデオ信号を含む第2フィールドと、を含む一連のテレビジョンフィールドを含むビデオ番組を記録するビデオ記録媒体。

【請求項13】　複数のコード暗号化キーが1つの番組に対して使用され、所望するコード暗号化キーが、前記所望するコード暗号化キーによって暗号化されたランダムディジタルコードに対応するコード暗号化キー識別データによって前記複数のコード暗号化キーから選択され

る、請求項１２記載のビデオ記録媒体。

【請求項１４】　前記第２フィールドが、コード暗号化キーによって暗号化されたランダムディジタルコードと番組識別データとの両方を含む垂直帰線消去時間を有し、かつ、前記第２フィールドの前記ランダムディジタルコードによって前もって視聴可能なビデオ信号から変換された視聴不可能なビデオ信号を含む第３フィールドが続く、請求項１２記載のビデオ記録媒体。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明はビデオ制御システムに関する。後で、視聴することが制御されるような、暗号化された放送またはビデオ画像の収録複写物を復号化するビデオ制御システムを提供することが望まれている。このことは所有者が自由に、視聴することを禁止するか、あるいは収益を回収するかを可能とする。

【０００２】

【従来の技術】従来技術においては、コンピュータプログラムが一度ダウンロードされると、それぞれの続いて起こるそのプログラムの使用においては、アクセス・キーで、使用することが可能となるようなソフトウェア分配システムが知られている。このシステムは、ＩＤと内部のダイナミック・カウンタとの両方で使用者の復号器ボックスに直接に関連づけられる絶えず変化する、ダイナミック・キーを使用する。

【０００３】また、２４時間かまたは一度だけかで収録物を視聴することを自主的に制御するビデオシステムが知られているが、それは所望される制御能力を有しない。

【０００４】

【発明が解決しようとする課題】視聴することが制御されるような、暗号化された放送またはビデオ画像の収録複写物を復号化するビデオ制御システムを提供する。

【０００５】

【課題を解決するための手段】簡単にいうと、中央機構と端末を備えたビデオシステムである。ビデオ番組手段が、コード暗号化キーによって暗号化されたランダムディジタルコードと、番組識別データの両方を含む第１フィールドと、そのランダムディジタルコードによって視聴ないし理解できるビデオ信号から前もって変換された視聴できないビデオ信号を含む第２フィールドと、を含む一連のテレビジョンフィールドを含むビデオ番組を端末に提供する。端末は、番組識別データを中央機構に送信する手段を備える。中央機構は、番組識別データに対応する少なくとも１つのコード暗号化キーを記憶し検索するデータベースと、中央機構から端末へコード暗号化キーを送信する手段とを備える。端末は、さらに、中央機構からのコード暗号化キーを受信する手段と、コード暗号化キーによって暗号化された第１フレームのディジタルコードを復号化する復号化手段と、復号化されたランダムディジタルコードを用いて第２フレームの視聴できないビデオ信号を視聴できるビデオ信号に変換する手段と、を備える。ビデオ番組手段は、端末へ番組を送信してもよいし、あるいは、端末に配置されて番組を収録したビデオ記録媒体を再生してもよい。番組を収録するビデオ記録媒体もまた、本発明において請求される。

【０００６】

【実施例】本発明の実施例であるビデオシステム１０の概略ブロック図である第１図を参照すると、ビデオシステムは、中央機構１１と、端末１２と、そして中央機構１１と端末１２との間の全二重通信リンク１３と、を備えている。システムの外観がまず第１に掲げられている。

【０００７】端末１２に、コード暗号化キーによって暗号化されたランダムディジタルコードと番組識別データとの両方を含む第１フィールドと、ランダムディジタルコードによって視聴できるビデオ信号から前もって変換された視聴できないビデオ信号を含む第２フィールドと、を含む一連のテレビジョンフィールドを含むビデオ番組が提供される。

【０００８】ビデオ番組は、放送、ケーブル、衛星、光ケーブル、あるいは他のいかなる伝送メディア、１４によって送信されてもよい。代わりに、ビデオ番組は、磁気テープあるいはビデオディスクのようなビデオ記録媒体１５に記録され、記録／再生装置１６によって再生されてもよい。視聴できないビデオ信号は、アナログあるいはディジタルのいずれであってもよい。

【０００９】第２フィールドは、コード暗号化キーによって暗号化されたランダムディジタルコードと番組識別データとの両方を含み、かつ、その次に第３フィールドが続く。その第３フィールドは、第２フィールドのランダムディジタルコードによって視聴できるビデオ信号から前もって変換された視聴できないビデオ信号を含む。

【００１０】端末１２は、端末識別データを記録する手段１７と、リンク１３を介して中央機構１１へ端末識別データと番組識別データを送信する手段とを備える。

【００１１】中央機構１１は、番組識別データに対応する少なくとも１つのコード暗号化キーを記録し検索するデータベース１９と、中央機構１１から端末１２へコード暗号化キーを送信する手段２０と、端末識別データと番組識別データの両方に基づいて課金データを生成する手段２１と、を備える。

【００１２】端末１２は、さらに、中央機構１１からのコード暗号化キーを受信する手段２２と、コード暗号化キーによって第１フレームの暗号化されたランダムディジタルコードを復号化する復号化手段２３と、復号化されたランダムディジタルコードを用いて第２フレームの視聴できないビデオ信号を視聴できるビデオ信号に変換する手段２４と、を備える。

【００１３】それぞれの端末１２は、端末に特有の暗号

化キーと、番組識別データ、および端末に特有の暗号化キーによって暗号化された端末１２の識別データを中央機構に送信する手段１８と、を有してもよい。中央機構１１は、端末に特有の暗号化キーの複製を記録する手段と、端末に特有の暗号化キーによってコード暗号化キーを暗号化する手段と、中央機構１１から端末１２へ暗号化されたコード暗号化キーを送信する手段と、を有する。

【００１４】端末１２は、さらに、中央機構１１からの暗号化されたコード暗号化キーを受信する手段２２と、端末に特有の暗号化キーによってコード暗号化キーを復号化し、そしてコード暗号化キーによって第１フレームの暗号化されたランダムディジタルコードを復号化する復号化手段２３と、復号化されたランダムディジタルコードを用いて第２フレームの視聴できないビデオ信号を視聴できるビデオ信号に変換する手段２４と、を備える。

【００１５】端末１２は、、端末に特有の暗号化キーによって端末識別データを暗号化する手段と、暗号化されない端末識別データと暗号化された端末識別データを中央機構に送信する手段と、を備え、そのことは、中央機構が、端末の同一性を検査するために暗号化されない端末識別データと暗号化された端末識別データを比較する手段を含むことでもある。

【００１６】複数のコード暗号化キーが１つの番組に使用されてもよく、ここでは、ランダムディジタルコードに対応するコード暗号化キー識別データによって複数のコード暗号化キーの中から所望のコード暗号化キーが選択される。

【００１７】システムの種々の態様をここでさらに詳しく論述する。

【００１８】システム１０がビデオ番組を視聴することを制御する。ここでビデオ番組とは、一連の走査線のフィールドからなるテレビジョンフォーマットで転送されるかあるいは記録されるあらゆるビデオ画像を意味する。飛越し走査における２つのフィールドが１つのテレビジョンフレームを組み立てる。

【００１９】ビデオ番組は、あらゆるアナログあるいはディジタルの方法によって、例えば、スクランブル操作されて(scrambled)、視聴できないようにされ、そして、フィールドに配置されたランダムディジタルコードを用いて、例えば、スクランブルを回復せしめられて(descrambled)、視聴できるようにされる。ランダムディジタルキーはそれら自身が暗号化され、視聴するときに使用者に固有の情報とともに、中央機構に配置されたデータベースから得られる少なくとも１つのキーによって、復号化される。システムは、複写を停止させることはない。すなわち、収益を保護しつつ視聴することを制御するのである。つまり、複写することを推奨できる。それにより、収益が再生の度に集金され得るように再生することを制御することによって分配の問題は容易化されよう。

【００２０】好ましくは、全二重リンク１３は、ＩＳＤＮのＤチャネルのような、あるいは標準電話回線を介するモデムによる、端末と中央機構間の継続的なデータ回線である。

【００２１】ビデオ番組は暗号化され、そして、端末で視聴するには復号器が必要とされる。その復号器は、データアクセスとともにビデオ番組に組み込まれたデータを使用して、復号化を正確に行い、ゆえに、処理が完全に制御される。遠隔のデータベースからのその組み込まれたデータとキーの転送は、最初の視聴以前に高度の安全性が提供されるならば公開されている暗号化技法で保護されてもよい。

【００２２】ビデオ番組は、そのまま収録されてもよいが、依然としてそれは視聴することができないものである。それを視聴するには、暗号化された組み込まれたデータと、保護されたデータベースへのアクセスとともに、復号器が使用されて、復号化を行う。収録したものは自由に複写されるかもしれないが、その復号器を使用しない限り、視聴することができないままのものである。

【００２３】ビデオ番組を視聴するためには、暗号化されたデータ転送を用いて、データベースにアクセスする必要がある。この過程では、結果として、収録であれ送信であれ、ビデオ番組の制御を生じることとなる。復号器はデータベースから到着する少なくとも１つのキーを必要とする。キーを得るためには、ビデオ番組からの情報と端末の識別がデータベースに送信される。

【００２４】電子的資金移動(EFT：electronic funds transfer)による直接の支払いが、その情報を用いて行われる。その番組がビデオショップの複写であれば、EFTにはビデオショップ料金と著作権料が含まれる。ビデオショップへのビデオの配給は取るに足らないことであることに注意されたい。なぜなら、彼らは、彼らの認可された変換ボックスとともにビデオショップキーを用いて、直接収録することと、彼らが好きなだけ複写したものを作ることを勧められているからである。視聴している時間に収益管理が行われる。このため、分配形態の配給(sharewaretype of distribution)が勧められる。

【００２５】パス・キーがデータベースに送信され、成人向けのフィルムを視聴することを可能とし、未成年者によるアクセスを制御することができる。

【００２６】最初のアクセスにおいて、データベースは、使用者の装置とビデオ収録物から得られるサイン(signature)を取り出し、その後の追跡のためにそれを記録する。この過程でデータベースに強制的なアクセスがなされるので、使用に関するデータが収集される。これと同様の処理が収益を回収することにも使用される。

7

【００２７】システムは、好ましくは、少なくとも１つのダウンロード可能なキーと、そのキーを復号化に使用する暗号化されたビデオ番組と、ビデオ番組のフィールドに記録されたデータと、を使用する。それは、ディジタル、アナログ、あるいはアナログとディジタルが混合された、あらゆる環境において実行されてよい。

【００２８】ビデオ番組は、例えば、それが転送された場所、時、相手のような、番組に関係するデータで暗号化される。そのデータはまた復号化キーの一部を含んでもよい。この情報が信号から抽出され、データベースにアクセスするのに使用され、番組の所有者によって保持され、復号器のための暗号化キーが得られる。加入者の、そして（あるいは）信用の検査が首尾よく完了した後に、１つあるいはそれ以上のキーが転送される。この時点で、所有者は、特定のユーザＩＤによって利用データを得、所有者に対する課金を選択する自由を有する。もしそれが無料の番組であれば、少なくともその視聴者のデータは手に入れることができる。

【００２９】もし使用者が、転送されるもの、あるいは他の収録物を記録するのであれば、上述したように、組み込まれたデータとともに、暗号化された信号を得ることとなる。このことは、処理過程でのサインをなす部分を達成する。この方法によって生成される収録物は、標準のＶＣＲ（video cassette recorder ）であってもよいが、暗号化され個別にマーキングされる。収録物を複写することはシステムには影響しない。なぜなら、再収録は正しいキーによって有効なだけであるからである。可能性として、番組の最初の数分はキーを必要とせずに視聴することが可能であってもよく、データベースのためにアクセスとキーの同期処理のための時間を許容するとともに、ユーザが番組の内容が何なのか確認することを可能とする。

【００３０】収録物を再生するためには、少なくとも１つのキーを再度得ることが必要である。フィールドに記録されたデータの組み合わせがデータベースへのアクセスに使用される。キーが利用可能にされる以前には、端末識別と組み込まれたデータが一致するか検査される。

【００３１】収録物がビデオショップで借りられたものである場合、コードがその店を識別してもよい。データベースはその収録物をレンタルビデオの複写物として認識し、ユーザかあるいはビデオショップに料金を課す。もし収録物が２回視聴されればその課金が反復される。複写がなされた場合、それが再生された時に、データベースは、実際に複写した者ではなく、元のビデオショップを識別する。しかしながら、貸出時に確認がなされれば、ある程度の制御がなされる。もし、全体の課金処理が、視聴者がすべての課金の責任を持つように、先方払いにされれば、分配（shareware ）により、複写することが推奨され、収益が使用料に基づいて保持されるとともに、配給の問題は最小限にとどめられる。

8

【００３２】番組の所有者は、その番組を配給することに携わるいかなる者に対しても支払が保証された複写物を用意する責任がある。その番組は、暗号化され、視聴者がその番組を利用できるようにデータベースを更新することを要求する。視聴者は復号器を含む端末を有し、中央機構のデータベースに自動ダイアルでリンクされ、接続できたら、ビデオ番組を復号化する。適切に、統計が取られ、データベースから信用の調査と請求がなされる。

【００３３】暗号化には２つのレベルがあり、１つは番組のビデオ復号化コードを保護するためのもので、もう１つは、端末と中央機構との間のメッセージの保護のためのものである。両方とも、ＮＢＳデータ暗号化標準（DES : Data Encryption Standard）を使用してもよい。

【００３４】ＤＥＳ暗号化／復号化は、端末で、そして中央機構で、商業的なモトローラ６８５９データ保護デバイスかあるいはそれに類似するものでなされてもよい。

【００３５】復号化コードそれ自体は、ＤＥＳ暗号化されることによって保護される。復号化キーはビデオ番組に存在するのではなく中央機構のデータベースに保持される。番組識別番号と復号化番号は、中央機構が復号化キーそれ自体に到達することを可能とし、それを端末に送信し復号化コードを復号化する。

【００３６】それぞれのフィールドに対して、異なったＤＥＳ暗号化キーは必要とされない。１つのキーがいくつかのフィールドに及ぶことができる。端末からのＤＥＳキーの要求とその応答はまた、中央機構への生存通知として作用してもよい。

【００３７】ＤＥＳ復号化キーは、高レベルＤＥＳ「セッション」キーによって保護されて、中央装置から端末へ転送される。テープ走行はまたＤＥＳセッションキーによって保護されているので、端末は新しいキーを要求する。このキーは、そのセッションが開始されたときに中央機構によって生成され、そのセッションの間は有効のままである。端末は、ＲＯＭに記録された端末固有のＤＥＳキーを使用してそのセッションを開始する。

【００３８】フレームの内容が、アナログ・サブシステムからＤＣＳＳに転送され、復号化された復号化コードがＤＣＳＳからアナログ・サブシステムへ図示されるアナログインタフェースを介して転送される。サブシステム間のデータの転送は、垂直水平帰線消去信号とそれらにより誘導される中断よって調整されてもよい。

【００３９】端末と中央機構との間のすべてのメッセージは、周期冗長検査コード（ＣＲＣ：Cyclic Redundancy Code）を用いてメッセージの完全性を確認する。ＣＲＣ－ＣＣＩＴＴ生成多項式は、各メッセージに対して２つのブロック検査文字（ＢＣＣ）を生成する。端末が、ＢＣＣによって完全性のないメッセージを受信した場

合、端末はその最後のメッセージを再送するように中央機構に再送要求（ＡＲＱ）を送信する。中央機構はＡＲＱの不完全なメッセージの再送要求は試みない。それは放棄され、端末が再送するのを待つ。

【００４０】音声呼出方式（ＶＣＳ）でのメッセージのやり取りは、ある種の応答が、送信されるそれぞれのメッセージによってなされる肯定応答体系による。例えば、端末は、ＤＥＳ復号化キーメッセージの要求を送信した後、ＤＥＳ復号化キーメッセージを期待し、中央機構は、キーメッセージを送信した後、キー受信応答を期待する。

【００４１】ユーザが保護された番組の再生を開始するとき、端末は、「セッション開始」メッセージ（ＳＴＳ：session start message）を、ユーザと番組の識別を含む中央機構に送信することによって、１つのセッションを開始する。メッセージは、メッセージの種別と、ユーザ番号と、ＣＲＣコードとを、暗号の形態でなく平文で含むが、そのメッセージの残部は、端末のＲＯＭに格納された最初のＤＥＳセッションキーによってＤＥＳ暗号化される。（ユーザ識別もまたＲＯＭに格納されている。）中央機構は、暗号化されないデータを用いてそのデータベースにアクセスし、メッセージの残りの部分を復号化するためのユーザＤＥＳの値を検索する。

【００４２】中央機構は、純粋な番号および復号化されたユーザ番号とを比較することによってメッセージを検証する。そのユーザ番号が同一である場合には、中央機構は番組一連番号が正当か確認する。中央機構はまた、ユーザの信用を検査してもよい。すべてが良ければ、中央機構はそのセッションを受け入れてそのセッションに固有の新しい（かつ無作為の）ＤＥＳキーを生成する。中央機構は、データベースの最初のユーザ値を用いてこれを暗号化し端末に送信する。それは、メッセージを復号化し、その新しい値をそのセッションの残りに対するセッションキーとしてデータベース（ＭＣＵ　ＲＡＭ）に格納する。

【００４３】中央機構は、ＳＴＳメッセージ内のテープ番号と復号化キー番号を用いて、データベースから番組に対する１組のＤＥＳ復号化キーを検索する。これらは、セッションキーによって暗号化され、セッションの

開始時かあるいはセッションの間中に、端末に送信される。

【００４４】端末は、セッション開始メッセージと、応答メッセージと、ＡＲＱメッセージとを生成する。中央機構が、本来の性質において、応答する。中央機構および端末の両方が、ブロック検査文字を生成しかつ検査する。

【００４５】本発明の好ましい実施例と最良の態様が記述されたが、この分野に精通した者には別法が容易に考えられるであろう。したがって、本発明は特許請求の範囲で定義されるものであって、上述の特定の実施例によって定義されるものではない。

【００４６】

【発明の効果】視聴することが制御されるような、暗号化された放送またはビデオ画像の収録複写物を復号化するビデオ制御システムを提供する。このことは所有者が自由に、視聴することを禁止するか、あるいは収益を回収するかを可能とする。

【図面の簡単な説明】

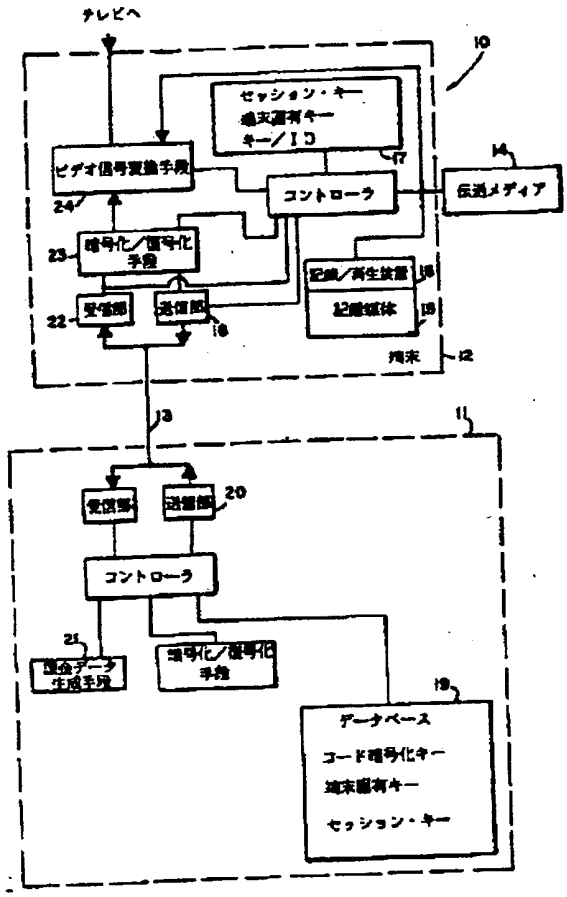
【図１】本発明を具体化したビデオシステムの概略ブロック図である。

【図２】本発明による暗号化の構成図である。

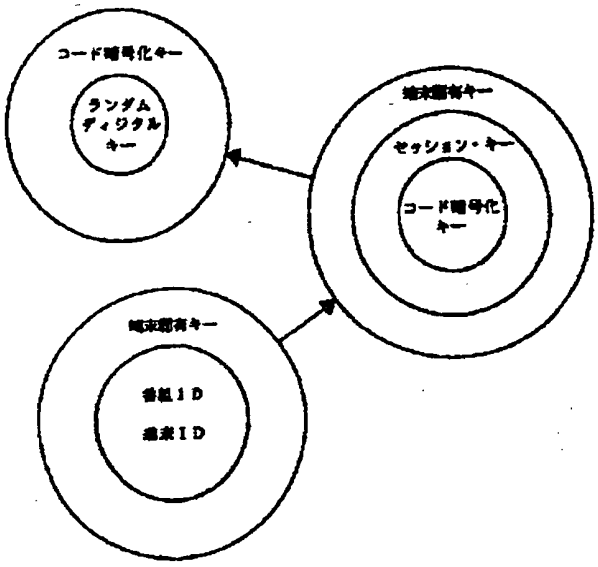
【符号の説明】

１０　ビデオシステム
１１　中央機構
１２　端末
１３　全二重通信リンク
１４　伝送メディア
１５　ビデオ記録媒体
１６　記録／再生装置
１７　記録手段
１８　送信手段
１９　データベース
２０　送信手段
２１　課金データ生成手段
２２　受信手段
２３　復号化手段
２４　ビデオ信号変換手段

【図1】



【図2】



フロントページの続き

(31)優先権主張番号　５０１６８４
(32)優先日　1990年３月29日
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　５０１６８５
(32)優先日　1990年３月29日
(33)優先権主張国　米国（ＵＳ）

(31)優先権主張番号　５０１６８８
(32)優先日　1990年３月29日
(33)優先権主張国　米国（ＵＳ）
(72)発明者　メルビン・ジエイ・テアー
米国マサチユーセツツ州フラミンガム、ウツドリー・ロード21